HW #2, DUE 1-20

MATH 505A

1. Let K be a finite abelian extension of $\mathbb{Q}$ (i.e. a finite Galois extension with abelian Galois group), regarded as a subfield of the complex numbers. Let $\alpha \in K$ be an algebraic integer whose complex norm is 1. Show that α is a root of 1, by first showing that all Galois conjugates of α also have norm 1, as do all Galois conjugates of all powers of α, and then arguing that all powers of α are roots of some monic polynomial with bounded degree and bounded integral coefficients; thus all such powers are roots of one of finitely many polynomials $p_1, \ldots, p_m$ over $\mathbb{Z}$. Deduce that all entries in the character table of a finite group with complex norm 1 are roots of 1.

2. Let L be a finite cyclic extension (Galois with a cyclic Galois group G) of a field K. Show that there is $\alpha \in L$ such that the G-conjugates of α form a K-basis of L. (Let g be a generator of G, say with order n. Then g is in particular a K-linear transformation from L to itself of order n. Use the invariant factor decomposition of such a transformation to write L as a direct sum of quotients $K[x]/(p_1), \ldots, K[x]/(p_m)$ as a $K[x]$-module, where $p_1 | p_2 | \cdots | p_m$; finally use the linear independence of the elements of G as linear transformations of L to show that $m = 1$ and $p_m = x^n - 1$.)

3. Show that the polynomial $x^{p^n} - x - 1$ is irreducible over the field $\mathbb{Z}_p$ for p prime if and only if either $n = 1$ or $n = p = 2$. (This polynomial is irreducible if and only if the Galois group of its splitting field acts transitively on its roots; a generator for this Galois group is the Frobenius automorphism of its splitting field.)

4. Let α be a root of an irreducible polynomial of degree 4 over $\mathbb{Z}_3$. Determine the other roots of this polynomial in terms of α; the answer does not depend on the choice of polynomial.

5. Show that the polynomial $x^4 + 1$ is irreducible over $\mathbb{Z}$ or $\mathbb{Q}$ but reducible over $\mathbb{Z}_p$ for any prime p, by looking at elements of order 8 in a suitable extension of $\mathbb{Z}_p$.